PCT/JP2004/011783

25. 8. 2004

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　８月１８日

出願番号
Application Number: 特願２００３－２９４０５６

[ST. 10/C]: [ＪＰ２００３－２９４０５６]

出願人
Applicant(s): サイエンスパーク株式会社

２００４年　９月３０日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号　出証特２００４－３０８７４５７

【書類名】　特許願
【整理番号】　PSP03002
【あて先】　特許庁長官殿
【国際特許分類】　G06F 13/10
G06F 13/38
【発明者】
【住所又は居所】　神奈川県座間市入谷４丁目３０１１番地の６　東建座間ハイツ２－５０９　サイエンスパーク株式会社内
【氏名】　小路　幸市郎
【発明者】
【住所又は居所】　神奈川県座間市入谷４丁目３０１１番地の６　東建座間ハイツ２－５０９　サイエンスパーク株式会社内
【氏名】　野▲崎▼　隆
【特許出願人】
【識別番号】　501180263
【氏名又は名称】　サイエンスパーク株式会社
【代理人】
【識別番号】　100093687
【弁理士】
【氏名又は名称】　富崎　元成
【選任した代理人】
【識別番号】　100106770
【弁理士】
【氏名又は名称】　円城寺　貞夫
【選任した代理人】
【識別番号】　100107951
【弁理士】
【氏名又は名称】　山田　勉
【手数料の表示】
【予納台帳番号】　012911
【納付金額】　21,000円
【提出物件の目録】
【物件名】　特許請求の範囲　1
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1

【書類名】特許請求の範囲
【請求項１】
データを記憶するデータ記憶手段と、
認証用の識別データが登録されている識別データ記憶手段と、
ユーザの認証情報を入力する入力手段と、
前記入力手段からの入力データと、前記識別データ記憶手段に登録された前記識別データとを比較して前記ユーザの認証を行う認証手段と、
電子計算機と接続して前記データの送受信を行うインターフェース手段と
を備え、
前記認証の結果、前記入力データと前記識別データが一致するときに前記データへのアクセスを許可する電子データ管理装置において、
制御プログラムを記憶するプログラム記憶手段を有し、
前記認証手段によって前記ユーザが認証された後、前記制御プログラムが前記電子計算機にインストールされ、前記電子計算機から前記データを読み出しすることが可能になる
ことを特徴とする電子データ管理装置。
【請求項２】
請求項1において、
前記認証手段による前記認証が完了した後、前記電子データ管理装置のロックが解除されて、接続されている前記電子計算機が前記電子データ管理装置の自動認識を開始する
ことを特徴とする電子データ管理装置。
【請求項３】
請求項１又は２において、
前記データ記憶手段と前記プログラム記憶手段とをスイッチするスイッチ制御手段を有し、
前記スイッチ制御手段は、前記プログラム記憶手段と接続されていて、前記ユーザ認証が行われ、前記制御プログラムが前記電子計算機にインストールされた後、前記データ記憶手段側にデータ読み取りを切り替えする
ことを特徴とする電子データ管理装置。
【請求項４】
請求項１ないし３から選択される１項において、
前記電子計算機から前記データ記憶手段に書き込みすることが可能で、前記データを用いて前記電子計算機で操作した履歴又は前記電子計算機を操作した履歴が前記データ記憶手段に書き込まれる
ことを特徴とする電子データ管理装置。
【請求項５】
請求項１ないし４から選択される１項において、
前記識別データは指紋データであり、
前記入力手段から前記ユーザの指紋情報を入力し、
前記認証手段では前記ユーザの指紋認証を行う
ことを特徴とする電子データ管理装置。
【請求項６】
請求項１ないし４から選択される１項において、
前記識別データは登録暗証番号であり、
前記入力手段から暗証番号を入力し、
前記認証手段では前記暗証番号と前記登録暗証番号と比較して前記ユーザの認証を行う
ことを特徴とする電子データ管理装置。
【請求項７】
請求項１ないし４から選択される１項において、
前記認証手段は錠と鍵を有し、
前記鍵を持っている前記ユーザに前記データへのアクセスを許可する

ことを特徴とする電子データ管理装置。
【請求項８】
登録された認証用情報を記憶する認証用情報領域と、
ユーザの識別情報を入力する入力部と、
前記認証用情報と、前記入力部から入力された前記入力情報とを比較して前記ユーザの認証を行うための認証機能を有する認証部と、
データを記憶するデータ記憶領域と、
制御プログラムを記憶するプログラム記憶領域と
を有し、
電子計算機と接続されると前記認証部によって前記ユーザの前記認証を行い、前記認証が完了すると、前記ユーザには前記データ記憶領域にアクセスする許可を与える電子データ管理装置において、
前記認証が行われた後に前記制御プログラムが前記電子計算機にインストールされ、前記電子計算機で前記データを利用して作業を行うとき、前記作業の履歴を記憶するように前記電子計算機を動作させる
ことを特徴とする電子データ管理装置用制御プログラム。
【請求項９】
請求項８において、
前記電子計算機との前記接続が切断されると、前記制御プログラムが前記電子計算機内に送信された前記データを削除する
ことを特徴とする電子データ管理装置用制御プログラム。
【請求項１０】
請求項８又は９において、
前記制御プログラムが自動消滅する機能を有する
ことを特徴とする電子データ管理装置用制御プログラム。
【請求項１１】
請求項８ないし１０から選択される１項において、
前記制御プログラムは、
前記電子計算機で前記データを複製、削除、編集、閲覧、読み込み、書き出しから選択される一以上の履歴、又は前記データを用いて作成したファイル、データの履歴を取得する履歴取得機能と、
前記履歴を前記データ記憶領域に書き込みするデータ記録機能と、
通信手段を利用して前記履歴を送信する送信機能と
を有する
ことを特徴とする電子データ管理装置用制御プログラム。
【請求項１２】
請求項１１において、
前記履歴は、
前記電子計算機のキーボードから入力された入力履歴、又はマウスを操作した操作履歴である
ことを特徴とする電子データ管理装置用制御プログラム。
【請求項１３】
請求項８ないし１２から選択される１項において、
前記制御プログラムが前記データを前記電子計算機内に特定アプリケーションで又は任意に複製、削除、編集、閲覧、読み込み、書き出しする操作から選択される一以上の操作だけをできるように前記電子計算機のファイルシステムに制限をする
ことを特徴とする電子データ管理装置用制御プログラム。
【請求項１４】
請求項８ないし１３から選択される１項において、
前記制御プログラムがカーネルモードで動作する

ことを特徴とする指紋認証電子データ管理装置用制御プログラム。

【請求項１５】

電子データ管理装置が、

認証用情報を記憶する認証情報記憶部と、

ユーザの認証情報を入力する入力部と、

前記入力部からのデータ用いて前記ユーザの認証を行う認証部と、

データを記憶するデータ記憶部と

を有し、

電子計算機に接続されると前記認証部によって前記ユーザの前記認証が行われ、前記記憶部に登録されたデータと一致する前記認証情報を有する前記ユーザに前記データへのアクセスを許可する

データアクセス方法において、

前記電子データ管理装置が制御プログラムを格納するプログラム記憶部を有し、

前記認証が終わると前記制御プログラムが前記電子計算機にインストールされ、

前記電子計算機で前記データを利用する利用環境を確保する

ことを特徴とするデータ管理方法。

【請求項１６】

請求項１５において、

前記利用環境は、前記電子計算機で動作する特定アプリケーションプログラムからのみ前記データへアクセスすることを許可する制限である

ことを特徴とするデータ管理方法。

【請求項１７】

請求項１５又は１６において、

前記制御プログラムは、キーボードからの入力、マウス操作などの前記電子計算機を操作する履歴、又は前記データを用いて複製、削除、編集、閲覧、読み込み、書き出しする操作から選択される一以上の前記データへのアクセスの履歴、又は前記データを用いて作成したファイルの履歴を残す機能を有する

ことを特徴とするデータ管理方法。

【請求項１８】

請求項１５ないし１７から選択される１項において、

前記電子データ管理装置と前記電子計算機との前記接続が切断されると、前記制御プログラムは、前記電子計算機内の前記データ、前記データの複製、前記データを利用して作成したデータ又はファイルなどの内１つ以上を削除する

ことを特徴とするデータ管理方法。

【請求項１９】

請求項１５ないし１８から選択される１項において、

前記制御プログラムが自動消滅する機能を有する

ことを特徴とするデータ管理方法。

【書類名】明細書
【発明の名称】電子データ管理装置、その制御プログラム及びデータ管理方法
【技術分野】
【０００１】
本発明は、ユーザのデータを格納し、管理する電子データ管理装置、その制御プログラム、及びデータ管理方法に関する。詳しくは、電子計算機に接続して使用する電子データ管理装置、その制御プログラム、及びデータ管理方法に関する。更に詳しくは、生態情報、暗証番号、鍵等を利用して個人認証を行い、メモリに格納されているデータへのアクセスを許可する電子データ管理装置、その制御プログラム、及びデータ管理方法に関する。
【背景技術】
【０００２】
電子計算機にアクセスするときに、ユーザの認証を行っている。このユーザ認証には、ユーザ名とパスワードをキーボードから入力するパスワード式認証、人間の指紋、掌形、声紋、顔、虹彩等の生体情報を利用するバイオメトリクス認証がある。また、電子計算機と接続して利用する周辺装置を利用するときもユーザ認証を行うことができる。
【０００３】
特に、外部記憶デバイスへアクセスするとき、セキュリティ面からは、ユーザ認証が重要である。従来から、電子計算機の本体、その周辺装置の電源、ケースなどに暗証番号又は鍵付きのロックを設けているものがある。その暗証番号を知っているユーザ又はその鍵を所持しているユーザのみが利用することができる。
【０００４】
外部記憶デバイスで利用されている記憶メディアとしては、数多くの種類がある。代表的なものとしては、ハードディスク、ＭＯ、ＤＶＤ－ＲＡＭがあり、ギガバイト以上の大容量のメディアである。また、コンパクトフラッシュ（登録商標）やスマートメディア（登録商標）、メモリースティック（登録商標）等のフラッシュメモリは数十から数ギガバイト容量の記憶メディアである。
【０００５】
ユーザはこれらのメディアにデータを記録して別の場所で再生したり、作業を継続したりする他、必要に応じて他人にデータを渡すときも利用している。これらの外部記憶メディアを再生するデバイスがＵＳＢ（Universal Serial Bus）等のインターフェースで電子計算機に接続されて、記録データの送受信を行っている。例えば、マイクロソフト社（登録商標）の Windows Me（登録商標）、 Windows 2000（登録商標）、 WindowsXP（登録商標）の場合は、ＰｎＰ機能を利用して電子計算機に接続されたデバイスを自動認識している。
【０００６】
ＵＳＢインターフェースで電子計算機にデバイスを接続すると、ＰｎＰ機能が自動的にデバイスを認識して必要なドライバをインストールするか、又はドライバインストールの指示を画面に表示させて、ユーザはその指示に従ってドライバをインストールして、接続デバイスを利用できる環境を提供している。これにより、接続された外部記憶装置のデータを読み込んだり、外部記憶装置へデータを書き込んだりする。
【０００７】
電子計算機を利用しようとするとき、マウスの指紋認証部によって指紋認証を行うことができる。例えば、電子計算機に接続されているマウスに指紋認証機能を持たせたものとしては、特許文献１の「個人認証用マウス及びそのシステム」に開示している。その他の例としては、記憶メディアに指紋認証情報を設けている例がある。
【０００８】
例えば、特許文献２の「可搬性記録媒体および可搬性記録媒体の使用方法」においては、ＣＤ－ＲＷにアプリケーションソフトウェア、ユーザ認証プログラム、指紋認証エンジンと、利用者の指紋情報等を格納して、指紋照合によるユーザ認証、認証後のアプリケーションソフトウェアの利用を提供している。

【０００９】
また、特許文献３の「電子データ管理装置、方法及び記録媒体」には、電子帳簿システムに関し、磁気カードに登録された取引情報が入力されて電子帳簿ファイルの修正を行うものである。このとき、磁気カードに登録された指紋情報と、電子帳簿システムに接続されている指紋認証装置から入力された指紋情報と、電子帳簿システム内のデータベースに記録されている指紋情報がすべて一致するときにのみ電子帳簿ファイルの修正を許可している。

【特許文献１】特開２００１－１２５７３４　「個人認証用マウス及びそのシステム」

【特許文献２】特開２００１－２２９０１７　「可搬性記録媒体および可搬性記録媒体の使用方法」

【特許文献３】特開２０００－３５３２０４　「電子データ管理装置、方法及び記録媒体」

【発明の開示】
【発明が解決しようとする課題】
【００１０】
フラッシュメディアなどによってデータを運び、別の電子計算機で読み込んで使用する場合、又は他人に渡して利用してもらう場合がある。しかし、ユーザにとっては、一般的にデータは重要なものであり、これらのデータをそのまま第三者に渡すことは元より、電子計算機にも残したくない。例えば、印刷業者に頼んで印刷を行うとき、ユーザは印刷データをフレキシブルディスクやＣＤ－ＲＯＭなどの媒体に入れて提供することが一般的である。印刷業者がこれらのデータを利用して印刷した後は、媒体を戻しても、データが業者の電子計算機内に残ることになる。これはユーザにとってセキュリティの面では好ましくない。
【００１１】
本発明は上述のような技術背景のもとになされたものであり、下記の目的を達成する。
本発明の目的は、電子計算機と接続されると自動的にインストールされて電子計算機内のデータの制御を行うことができる制御プログラムを格納した電子データ管理装置、その制御プログラム、及びデータ管理方法を提供する。
本発明の他の目的は、電子計算機から切断されると電子計算機に送信された、または電子計算機内に加工されたデータ、作成されたファイル等を消去することができる制御プログラムを格納した電子データ管理装置、その制御プログラム、及びデータ管理方法を提供する。
【００１２】
本発明の更に他の目的は、電子計算機から切断されると自ら消滅することができる制御プログラムを格納した電子データ管理装置、その制御プログラム、及びデータ管理方法を提供する。
本発明の更に他の目的は、個人認証機能を有する電子データ管理装置、その制御プログラム、及びデータ管理方法を提供する。
【課題を解決するための手段】
【００１３】
本発明は、前記目的を達成するため、次の手段を採る。
本発明の第１の発明の電子データ管理装置は、データを記憶するデータ記憶手段と、認証用の識別データが登録されている識別データ記憶手段と、ユーザの認証情報を入力する入力手段と、前記入力手段からの入力データと、前記識別データ記憶手段に登録された前記識別データとを比較して前記ユーザの認証を行う認証手段と、電子計算機と接続して前記データの送受信を行うインターフェース手段と制御プログラムを記憶するプログラム記憶手段を有する。
【００１４】
電子データ管理装置は、前記認証の結果、前記入力データと前記識別データが一致する

ときに前記データへのアクセスを許可し、前記認証手段によって前記ユーザが認証された後、前記制御プログラムが前記電子計算機にインストールされ、前記電子計算機から前記データを読み出しすることが可能になると良い。

【００１５】

また、前記認証手段による前記認証が完了した後、前記電子データ管理装置のロックが解除されて、接続されている前記電子計算機が前記電子データ管理装置の自動認識を開始すると良い。

更に、前記データ記憶手段と前記プログラム記憶手段とをスイッチするスイッチ制御手段を有し、前記スイッチ制御手段は、前記プログラム記憶手段と接続されていて、前記ユーザ認証が行われ、前記制御プログラムが前記電子計算機にインストールされた後、前記データ記憶手段に切り替えをすると良い。

【００１６】

また更に、前記電子計算機から前記データ記憶手段に書き込みすることが可能で、前記データを用いて前記電子計算機で操作した履歴又は記電子計算機を操作した履歴が書き込まれると良い。前記識別データは指紋データで、前記入力手段から前記ユーザの指紋情報を入力し、前記認証手段では前記ユーザの指紋認証を行うと良い。

【００１７】

更に、前記識別データは登録暗証番号で、前記入力手段から暗証番号を入力し、前記認証手段では前記暗証番号と前記登録暗証番号と比較して前記ユーザの認証を行うと良い。更に、前記認証手段は錠と鍵を有し、前記鍵を持っている前記ユーザに前記データへのアクセスを許可すると良い。

【００１８】

本発明の第２の発明の電子データ管理装置用制御プログラムは、電子データ管理装置内に記録されている制御プログラムであり、電子データ管理装置は、制御プログラムを記憶するプログラム記憶領域を有し、前記認証が行われた後に前記制御プログラムが前記電子計算機にインストールされ、前記電子計算機で前記データを利用して作業を行うとき、前記作業の履歴を記憶するように前記電子計算機を動作させるプログラムである。

【００１９】

また、電子データ管理装置は、登録された認証用情報を記憶する認証用情報領域と、ユーザの識別情報を入力する入力部と、前記認証用情報と、前記入力部から入力された前記入力情報とを比較して前記ユーザの認証を行う認証機能を有する認証部と、データを記憶するデータ記憶領域とを有し、電子計算機と接続されると前記認証部によって前記ユーザの前記認証を行い、前記認証が完了すると、前記ユーザには前記データ記憶領域にアクセスする許可を与えると良い。

【００２０】

また、電子データ管理装置用制御プログラムは、前記電子計算機との前記接続が切断されると、前記制御プログラムが前記電子計算機内に送信された前記データを削除すると良い。更に、前記制御プログラムが自動消滅する機能を有すると良い。

更に、前記電子計算機で前記データを複製、削除、編集、閲覧、読み込み、書き出しした履歴、又は前記データを用いて作成したファイル、データの履歴を取得する履歴取得機能と、前記履歴を前記データ記憶領域に書き込みするデータ記録機能と、通信手段を利用して前記履歴を送信する送信機能とを有すると良い。

【００２１】

また更に、前記履歴は、前記電子計算機のキーボードから入力された入力履歴、又はマウスを操作した操作履歴であると良い。

前記制御プログラムが前記データを前記電子計算機内に特定アプリケーションで又は任意に複製、削除、編集、閲覧、読み込み、書き出しする操作のいずれか１以上の操作だけをできるように前記電子計算機のファイルシステムに制限をすると良い。電子データ管理装置用制御プログラムが前記制御プログラムがカーネルモードで動作すると良い。

【００２２】

本発明の第３の発明のデータ管理方法は、認証用情報を記憶する認証情報記憶部と、ユーザの認証情報を入力する入力部と、前記入力部からのデータ用いて前記ユーザの認証を行う認証部と、データを記憶するデータ記憶部とを有する電子計算機に接続され、前記認証部によって前記ユーザの前記認証が行われ、前記記憶部に登録されたデータと一致する前記認証情報を有する前記ユーザに前記データへのアクセスを許可するデータ管理方法であって、前記電子データ管理装置が制御プログラムを格納するプログラム記憶部を有し、前記認証が終わると前記制御プログラムが前記電子計算機にインストールされ、前記電子計算機で前記データを利用する利用環境を確保する。

【００２３】

また、前記利用環境は、前記電子計算機で動作する特定アプリケーションプログラムからのみ前記データへアクセスすることを許可する制限であると良い。

更に、前記制御プログラムは、キーボードからの入力、マウス操作などの前記電子計算機を操作する履歴、又は前記データを用いて複製、削除、編集、閲覧、読み込み、書き出しする操作から選択される一以上の前記データへのアクセスの履歴、又は前記データを用いて作成したファイルの履歴を残す機能を有すると良い。

【００２４】

また更に、前記電子データ管理装置と前記電子計算機との前記接続が切断されると、前記制御プログラムは、前記電子計算機内の前記データ、前記データの複製、前記データを利用して作成したデータ又はファイルなどの内１つ以上を削除すると良い。更に、前記制御プログラムが自動消滅する機能を有すると良い。

【発明の効果】

【００２５】

本発明によると、次の効果が奏される。

本発明は、電子計算機にインストールされてユーザデータの管理を行う制御プログラムを格納した電子データ管理装置を提供することによって、ユーザデータの正確な利用、セキュリティを向上させることが可能になった。

【００２６】

本発明は、電子計算機でユーザデータを利用して作業を行っても作業後データが残ることがないデータ管理を図ることができる。

本発明は、認証機能付きの電子データ管理装置を提供することによって、特定のユーザのみがアクセスできるようになった。

【発明を実施するための最良の形態】

【００２７】

〔実施の形態１〕

図１には、本発明の実施の形態１の概要を図示している。図１には、電子データ管理装置１の構成例の概要を図示している。電子データ管理装置１は、筐体２、筐体２の一面に設けた指紋情報入力部３、筐体２と接続されているコネクタ４から構成されている。図２には、筐体２に格納される基板５の構成の概要を図示している。

【００２８】

基板５の上には、第１メモリ６、第２メモリ７、ＵＳＢ（Universal Serial Bus）コントローラ９、中央演算装置（ＣＰＵ、Central Processing Unit）８等が配置されている。第１メモリ６は、ユーザのデータ及びファイル等のユーザデータを格納するためのメモリである。第２メモリ７は、制御プログラムを格納するためのメモリである。ＵＳＢコントローラ９は、コネクタ４を介して電子計算機（図示せず）との送受信を制御するためのプログラムである。ＣＰＵ８は、電子データ管理装置１全体を制御するための中央演算処理装置である。

【００２９】

電子データ管理装置１が電子計算機と接続され、制御プログラムが電子計算機にインストールされると、スイッチ１０が第２メモリ７から第１メモリ６へと切り替わり、ユーザデータの送受信が可能になる。また、基板５には、認証用データベース１１、認証モジュ

ール１２が配置されている。認証モジュール１２は指紋情報入力部３と連動してユーザの認証を行うためのものである。認証用データベース１１は、電子データ管理装置１を使用できるユーザの指紋情報等の識別データを格納したデータベースのためのメモリである。

【００３０】

図３は、電子データ管理装置１へこの識別データを記録する手順を示すフローチャートである。図３に図示したように、電子データ管理装置１を利用する前に、電子データ管理装置１へユーザデータを書き込み、ユーザの指紋情報を登録する。電子データ管理装置１へユーザデータを書き込みするための専用のアプリケーションプログラムがインストールされている電子計算機に、電子データ管理装置１を接続して、その専用のアプリケーションプログラムによってユーザのデータを電子データ管理装置１の第１メモリ６に書き込む（ステップ１）。

【００３１】

そして、電子データ管理装置１を利用するユーザの指紋情報などの識別情報を認証用データベース１１に登録する（ステップ２）。識別情報の登録が完了すると、電子計算機から電子データ管理装置１を抜き取って持ち出しが可能になる（ステップ３）。これらのユーザデータおよび、ユーザの指紋情報などの識別情報は、専用のファイルシステムを用いて行われても良い。

【００３２】

図４は、電子データ管理装置１を利用するときの全体の流れを図示したフローチャートである。電子データ管理装置１を電子計算機にＵＳＢコネクタを用いて接続する（ステップ１０）。電子データ管理装置１がユーザの指紋認証を行う（ステップ１１）。ユーザの指紋認証は、指紋情報入力部３からの指紋情報データを用いて認証モジュール１２が行う。

【００３３】

このとき、認証モジュール１２はユーザの指紋情報データを予め登録した識別データと比較して、「正当なユーザであるか？」を判定する（ステップ１２）。ユーザの指紋情報データが認証用データベース１１に格納されている識別データと一致しない場合は、「利用許可がないユーザ」と判定されて電子データ管理装置１を利用することができない（ステップ１３）。

【００３４】

ユーザの指紋情報データが認証用データベース１１に格納されているデータと一致する場合は、「正当なユーザである」と判定されて次の処理に移る。ＵＳＢコネクタ４のＰｎＰ機能が許可され開始する（ステップ１４）。第２メモリ７に格納されている制御プログラムが電子計算機にインストールされる（ステップ１５）。制御プログラムは電子計算機にインストールされて、ユーザがユーザデータを用いて作業できる環境を確保する。

【００３５】

制御プログラムのインストールが正常に行われたかの判定を行う（ステップ１６）。電子計算機、その上で動作するＯＳの設定によっては、外部からプログラム等のインストールができない場合がある。この場合は、制御プログラムのインストールが行われないので、電子データ管理装置１をこの電子計算機で利用することができない（ステップ１７）。

【００３６】

制御プログラムが正常にインストールされると、スイッチ１０が第１メモリ６への切り替えを行い、第１メモリ６を利用可能になる（ステップ１８）。第１メモリ６には、ユーザデータが保存されており、電子計算機へ転送することが可能になる。また、電子計算機上のアプリケーションプログラムから第１メモリ６へアクセスしユーザデータを呼び出すなどの作業を行うことができるようになる（ステップ１９）。

【００３７】

また、同時に電子計算機にインストールされている制御プログラムが、履歴情報などのデータを第１メモリ６に書き込むことができるようになる。履歴情報には、ユーザデータを利用した履歴、ユーザデータを利用して作成したファイルの履歴、キーボード入力、マ

ウス操作等の電子計算機を操作した履歴、電子計算機から周辺デバイス、通信回線を利用して行われたやりとりの履歴などが含まれても良い。ＵＳＢコネクタ４が切断されると（ステップ２０）、電子計算機にインストールされている制御プログラムが電子計算機内のユーザデータを削除する（ステップ２１）。

【００３８】

このとき、ユーザデータを利用し、加工して作ったデータ、ファイルの削除を行っても良い。そして、電子計算機にインストールされた制御プログラムが自動消滅する（ステップ２２）。このように、電子データ管理装置１の利用するとき、電子計算機上にはユーザデータが残ることがない。

【００３９】

電子データ管理装置１を利用するためには、予め利用できるユーザの識別情報を認証用データベース１１に登録しておく。電子データ管理装置１のデータは通常のインターフェースでアクセスできない状態になっている。電子データ管理装置１へのアクセスがロックされていて、ユーザ認証が正常に行われて、利用許可のあるユーザのみが電子データ管理装置１を利用することができる。そのとき、電子データ管理装置１のアクセスロックが解除されて、電子計算機へのアクセス、コネクタの接続が行われる。

【００４０】

〔実施の形態２〕

図５は、本発明の実施の形態２の概要を図示したフローチャートである。ユーザデータ、ユーザの指紋情報などの識別データが登録された電子データ管理装置１を使用する電子計算機に接続する（ステップ１００）。電子データ管理装置１がユーザの認証を指紋情報入力部３からの指紋情報データ用いて認証モジュール１２が行なう（ステップ１０１）。ユーザの指紋識別データを予め登録した指紋情報と比較して正当なユーザであるかを判定する（ステップ１０２）。

【００４１】

ユーザの指紋情報が認証用データベース１１に格納されているデータと一致しない場合は、利用許可がないユーザと判定され再度ユーザ認証が行われる（ステップ１０３）。これは、電子データ管理装置１が切断されるか、ユーザ認証が成功するまで続く。ユーザの指紋情報データが認証用データベース１１に格納されている識別データと一致した場合は正当なユーザであると判定され次の処理に移る。

【００４２】

電子データ管理装置１をアンロックにし（ステップ１０４）、ＰｎＰ機能が有効になり、ＰｎＰ機能が開始する（ステップ１０５）。ＰｎＰ機能を利用して、電子計算機が電子データ管理装置１を自動認識する。電子計算機が電子データ管理装置１を自動認識し終わると、通常の外付けメモリと同様にアクセスできるようになる（ステップ１０６）。電子データ管理装置１のＵＳＢコネクタを切断すると（ステップ１０７）、電子計算機との一連のデータの送受信が終了する。この実施の形態では、電子計算機に転送され、書き込まれたデータに関しては特別に制限を設けていない。電子データ管理装置１を持ち出してそれにアクセスできるユーザの認証を行ってからアンロックし、アクセス許可を行っている。

【００４３】

〔実施の形態３〕

図６には、本発明の実施の形態３の概要を図示している。本実施の形態３は、配布元と使用者からなるシステムに関し、使用者は配布元のデータを用いて作業を行い、その結果を配布元に報告するものである。また、配布元は提供するデータを特定の制限範囲だけに使用できる環境も提供している。

【００４４】

図６には、電子データ管理装置１（以下、ハードウェアという）を提供する配布元、それを使用する使用者とのやりとりの流れを図示している。配布元は、ファイルシステムの機能を拡張した拡張ファイルシステムを提供する（ステップ２００）。

【００４５】
拡張ファイルシステムは、使用者が利用したアプリケーションプログラムの履歴、データの読み取り・編集・書き込みの履歴、ファイルの読み込み・書き込み・複製・作成・削除などの履歴を取る機能を有する。また、電子計算機のファイルシステムが提供する機能を制限する機能も有する。更に、ユーザのキーボード入力の履歴、マウスのクリック等のマウスを操作する履歴を取る機能も有する。
【００４６】
使用者は、この拡張ファイルシステムを導入する（ステップ２０１）。配布元は、ハードウェアを提供する（ステップ２０２）。それと同時に、ハードウェアと連携して動作するユーティリティの提供も可能である。使用者は、使用するアプリケーションプログラムを配布元に申請し（ステップ２０３）、配布元はアプリケーションプログラムに対するハードウェア固有のファイルとデータを使用者に提供する（ステップ２０４）。
【００４７】
使用者は、これを受け取ってハードウェアを電子計算機に接続する（ステップ２０５）。ハードウェアが電子計算機に接続されてと、拡張ファイルシステムがハードウェアを認識し、制御モードに入る（ステップ２０６）。制御モードに関する情報は、配布元が提供したハードウェア固有のファイルに含まれている。
【００４８】
使用者が、配布元のデータを利用して作業を行う。これらの作業の履歴が記録される（ステップ２０７）。ファイル使用履歴は、ハードウェアに記録される（ステップ２０８）。作業が終了すると、「作業の完了」の通知を配布元に送信する（ステップ２０９）。配布元はこの「作業の完了」通知を受け取る（ステップ２１４）。
【００４９】
そして、履歴データを配布元に送信する（ステップ２１０）。配布元は、履歴データを受信し（ステップ２１５）、受信したら応答する（ステップ２１６）。拡張ファイルシステムがこの応答を受信したら、複製ファイル、作業ファイル、そのデータ等を削除する（ステップ２１１）。そして、制限モードを解除し、通常のファイルシステムのモードに入る（ステップ２１２）。
【００５０】
これらの一連の作業が終了すると、使用者はハードウェアを配布元に返す（ステップ２１３）。配布元は、履歴データを受信してから、使用者が履歴データを解析して（ステップ２１７）、提供ファイル、データを正確に使用したかを把握することができる。また、返却されてハードウェア内に保存されている履歴データを解析して把握することも可能である（ステップ２１８）。
【００５１】
使用者から配布元への履歴データなどの送信は専用通信回線、インターネット、公衆通信網などの通信網によって行われる。使用者と配布元は、通信網は通信網で接続されてない場合は、ハードウェアにそれらの履歴が保存されてハードウェアを返却することによって行われる。
【００５２】
〔実施の形態４〕
図７には、本実施の形態４の概要を図示している。本実施の形態４では制御プログラムが電子計算機にインストールされて、ユーザが使用するアプリケーションプログアムを登録できるようになっている。
【００５３】
電子データ管理装置１を電子計算機と接続してユーザ認証が行われる（ステップ３０１）。ユーザ認証が完了すると、電子データ管理装置１のアクセスロックが解除されて電子計算機とやり取りできるようになり、ＰｎＰ機能が有効になる。よって、電子データ管理装置１が電子計算機に認識されて、電子データ管理装置１のドライバのインストールが開始される（ステップ３０２）。電子データ管理装置１のドライバのインストール終了後は

、制御プログラムのインストールが開始される（３０３）

【００５４】

このとき、ユーザからアプリケーションプログラムの登録をすることが可能である（ステップ３０４）。ユーザはアプリケーションプログラムの登録をしない場合は、制御プログラムのインストールが続けて行われる（ステップ３０６）。ユーザがアプリケーションプログラムの登録を行う場合は、登録するアプリケーションプログラムを選択し、そのファイル名、パス、ディレクトリなどを指定、選択して登録を行う。（ステップ３０５）。

【００５５】

アプリケーションプログラムの登録が終わると、制御プログラムのインストールが続けて行われる（ステップ３０６）。制御プログラムが正常にインストールされたかを確認して電子データ管理装置１の使用が可能になる（ステップ３０７、３０８、３０９）。

【００５６】

また、上述のようにユーザが制御プログラムをインストールするときアプリケーションプログラムを登録し、その使用履歴を取得し、登録されたアプリケーションプログラムの使用範囲を制限することが可能である。アプリケーションプログラムの他に特定のデータ、ファイルを登録しても良い。データ、ファイルを登録すると、実施の形態１のようにデータ、ファイルの使用履歴を追跡して把握することが可能になる。ユーザは、制御プログラムを使用中でも、アプリケーションプログラム、データ、ファイルの登録、登録の取り消しすることも可能である。

【００５７】

〔実施の形態５〕

図８には、本発明の実施の形態５の概要を図示している。本実施の形態５では、電子データ管理装置１が切断されても制御プログラムを継続して使用可能なものを提供している。ＵＳＢコネクタが切断される（ステップ３５０）。そのとき、アンインストールを開始するかを確認する（ステップ３５１）。アンインストールしない場合は、電子データ管理装置１を継続して使用できる（ステップ３５６）。

【００５８】

アンインストールを開始するときは、今まで使用したデータを削除するかを確認し（ステップ３５２）、電子計算機内のデータを削除する（ステップ３５３）。そして、制御プログラム自身を削除するかを確認する（ステップ３５４）。データと制御プログラムを削除しない場合は、それぞれ続けて電子データ管理装置１を使用する（ステップ３５６）。ただし、制御プログラムの削除を行った場合は、継続して電子データ管理装置１を使用することができない（ステップ３５５）。

【００５９】

〔実施の形態６〕

本実施の形態６は電子データ管理装置１の他の実施の形態である。図９には、本実施の形態６の概要を図示している。電子データ管理装置２０は、筐体２、筐体２の一辺に設けた押しボタン式のキー２１、そしてコネクタ４から構成されている。

【００６０】

電子データ管理装置２０は、実施の形態１から５の電子データ管理装置１とはユーザ認証には暗証番号を利用している点が異なる。その他の機能は、前述した電子データ管理装置１と同様であり、詳しい説明は省略する。違っている部分の説明だけを行う。ユーザは、電子データ管理装置２０のロックを解除するために、その一辺に設けている押しボタン式のキー２１から暗証番号を入力する。

【００６１】

暗証番号を入力するときに、その入力開始、入力終了を識別するために「＃」、「＊」などの決められた記号キーを暗証番号入力の前後に押しても良い。押しボタン式のキー２１は０～９までの数字、一部の記号のボタンを有しているが、電子データ管理装置２０の大きさ、用途に合わせてボタンの数を増減しても良い。

【００６２】

電子データ管理装置２０の内部構造は図２と同様であり、ユーザ認証は認証モジュール１２が行い、その認証のためにはあらかじめ登録された暗証番号が認証用データベース１１に記憶されている。

【００６３】

この電子データ管理装置２０を利用するまでの手順は、図１０のフローチャートに示している。専用のアプリケーションプログラムでユーザデータを電子データ管理装置２０の第１メモリ６に書き込み、暗証番号を認証用データベース１１に登録する（ステップ４０１、４０２）。よって、電子データ管理装置２０が利用可能になる。

【００６４】

〔実施の形態７〕

本実施の形態７は電子データ管理装置１の他の実施の形態である。図１１には、本実施の形態７の概要を図示している。錠３２と鍵３１の組を用いたユーザ認証を行う電子データ管理装置３０の概要を図している。電子データ管理装置３０は、筐体２、筐体２の一辺に設けた錠３２、そしてコネクタ４から構成されている。錠３２を開閉するための鍵３１が１組になって付属する。電子データ管理装置３０の内部構造は図２と同様であり、ユーザ認証は認証モジュール１２が行う。ユーザ認証は、錠３２の開閉によって行われるので、認証用データベース１１が不要である。

【００６５】

実施の形態１から５の電子データ管理装置１とはユーザ認証に錠３２と鍵３１の組を利用している点が異なる。その他の機能は、前述の電子データ管理装置１と同様であり、詳しい説明は省略する。異なる部分の説明だけを行う。

【００６６】

ユーザは、電子データ管理装置３０のロックを解除するために、その一辺に設けている錠３２に矢印３３の方向で示すように鍵３１を差し込んで錠３２のロックを解除する。この情報を、認証モジュール１２が察知し、電子データ管理装置３０のアクセスロックを解除し、電子データ管理装置３０へのアクセスが可能になる。

【００６７】

本発明の実施の形態は、これまでに記述したような実施の形態１から７のみに適用され利用されるものではなく、同様な効果が得られ場どのような形式・形態でも利用しても良い。

【産業上の利用可能性】

【００６８】

本発明は、ユーザのファイルやデータなどを携帯可能なメモリ装置に記録して搬送して使用することが可能であり、セキュリティが必要な業界で利用すると良い。特に、営業または経理データ等でユーザデータやファイルなどの秘密情報の提供が必要とされる印刷業界、販売店で利用されることが望ましい。また、ペーパーレス処理を行うための機関、顧客へのファイル提供などに利用されても良い。音楽配信、映像配信、電子出版などの電子コンテンツ配信サービスを行うとき、被受信者を特定し、被受信者のメモリに電子コンテンツを書き込んで提供するときに利用されても良い。

【図面の簡単な説明】

【００６９】

【図１】図１は、電子データ管理装置１の構成例の概要を図示している図面である。

【図２】図２は、電子データ管理装置１の基板５の構成例を図示している概念図である。

【図３】図３は、電子データ管理装置１を利用する前の準備の手順を図しているフローチャートである。

【図４】図４は、電子データ管理装置１を利用する全体の流れを図示したフローチャートである

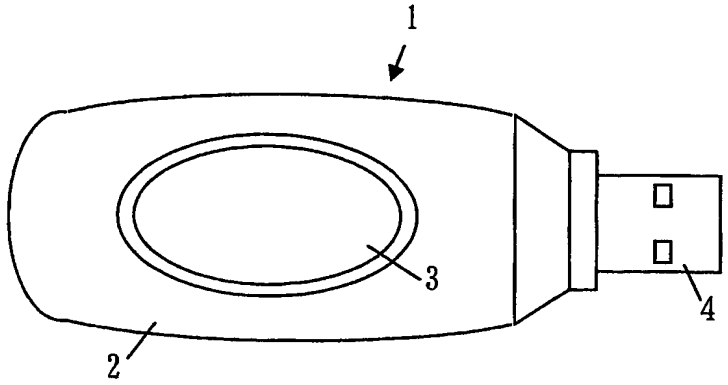
【図５】図５は、本発明の実施の形態２の概要を図示したフローチャートである。

【図６】図６は、本発明の実施の形態３の概要を図示したフローチャートである。

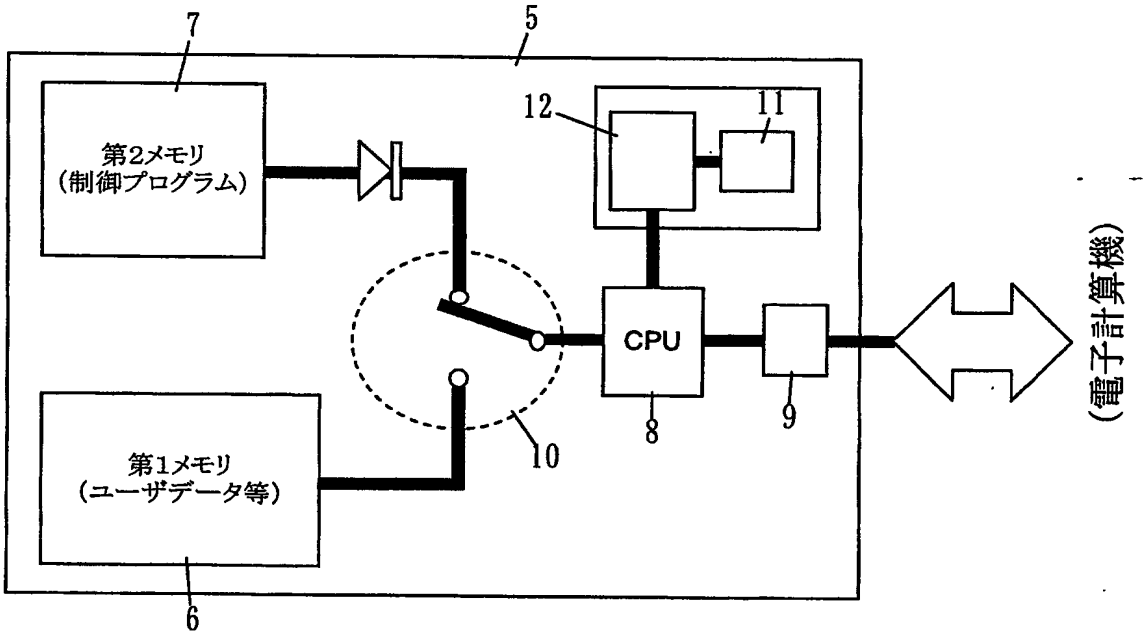
【図７】図７は、本発明の実施の形態４の概要を図示したフローチャートである。
【図８】図８は、本発明の実施の形態５の概要を図示したフローチャートである。
【図９】図９は、暗証番号を用いて認証を行う実施の形態６の概要を図示した図である。
【図１０】図１０は、電子データ管理装置２０の利用する準備の手順を図しているフローチャートである。
【図１１】図１１は、鍵を用いて認証を行う実施の形態７の概要を図示した図である。

【符号の説明】
【００７０】
１…電子データ管理装置
２…筐体
３…指紋認証部
４…ＵＳＢコネクタ
５…基板
６…第１メモリ
７…第２メモリ
８…ＣＰＵ
９…バスコントローラ
１０…スイッチ
１１…指紋認証用データベース
１２…指紋認証部
２０…電子データ管理装置
２１…押しボタン式入力部
３０…電子データ管理装置
３１…鍵
３２…錠

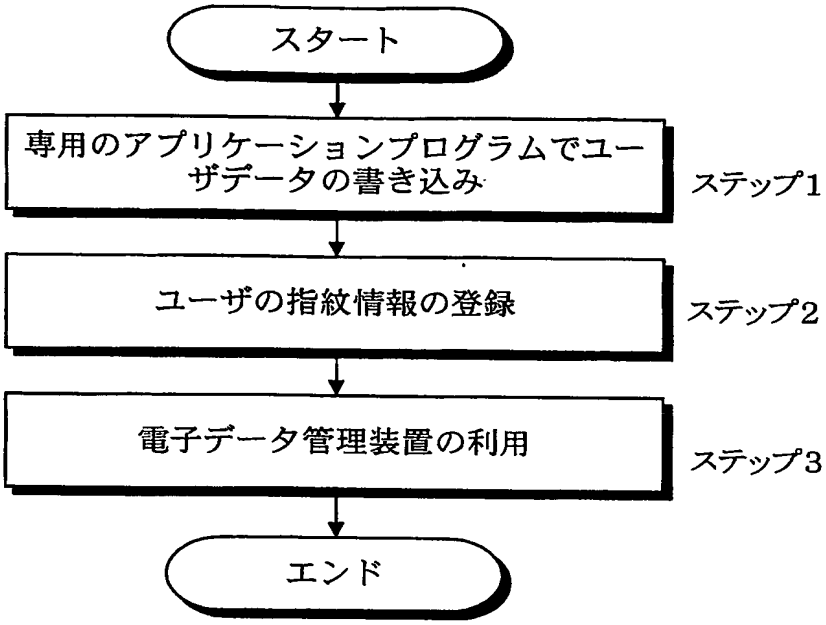
【書類名】図面
【図１】



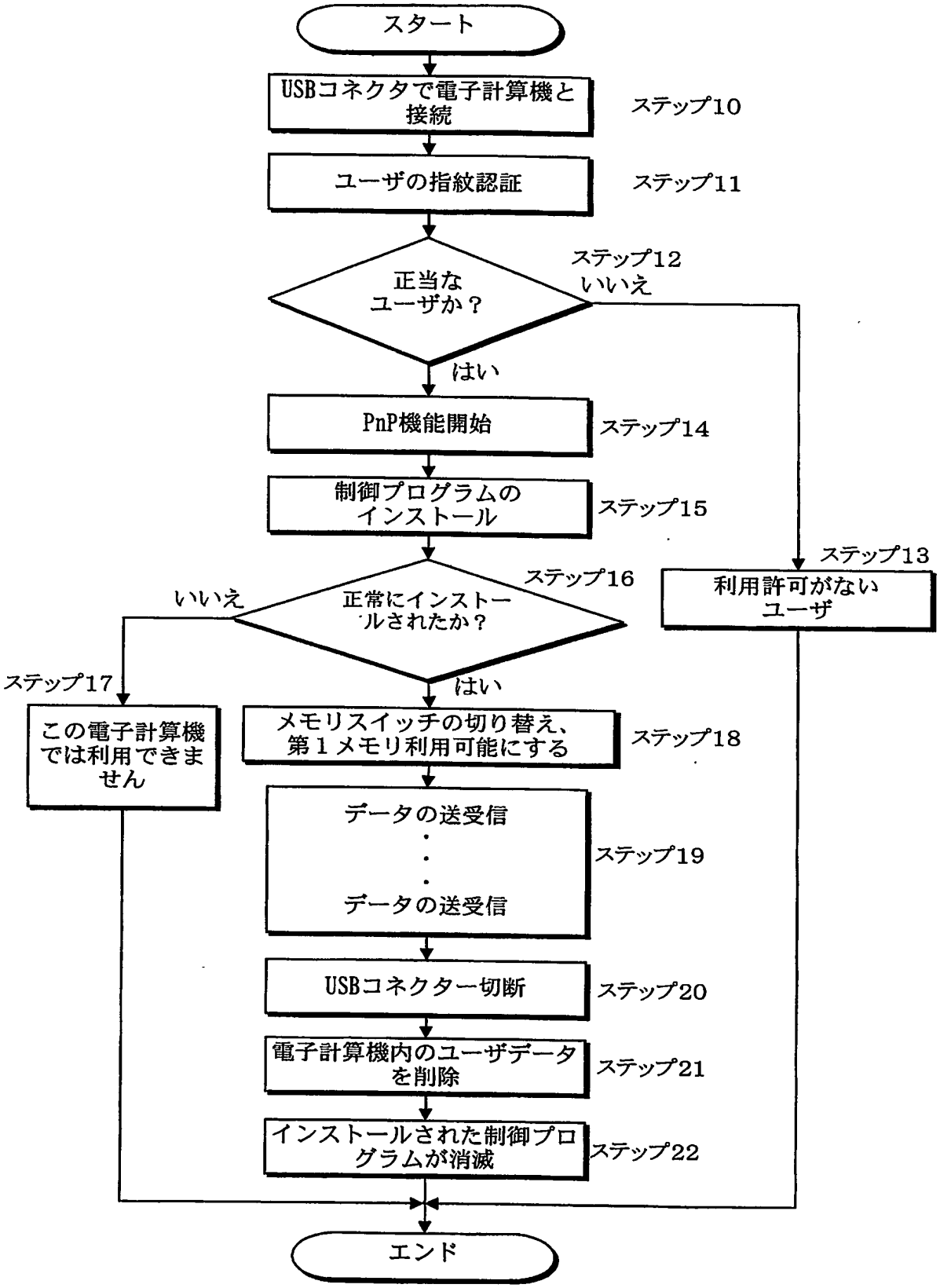
【図２】



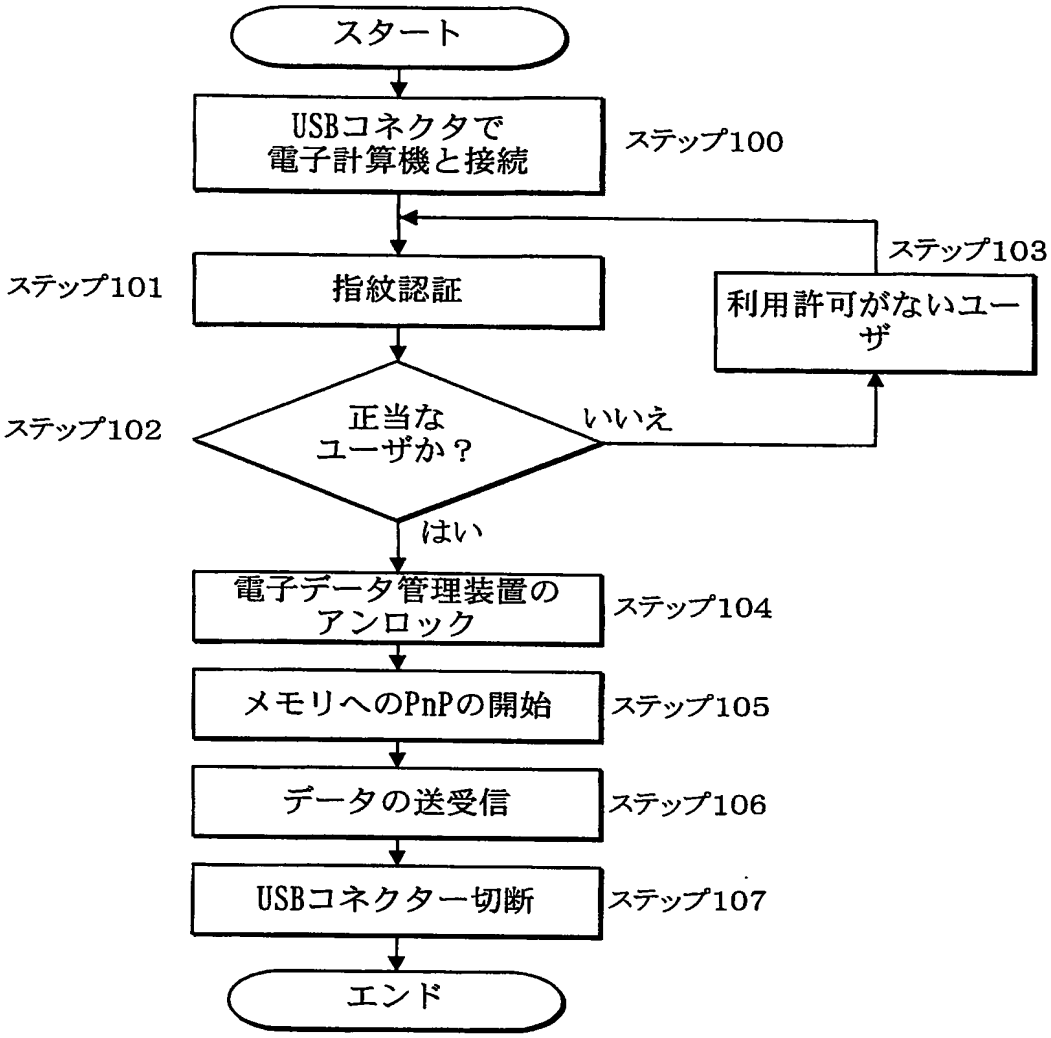
【図３】


スタート
専用のアプリケーションプログラムでユーザデータの書き込み
ステップ1
ユーザの指紋情報の登録
ステップ2
電子データ管理装置の利用
ステップ3
エンド

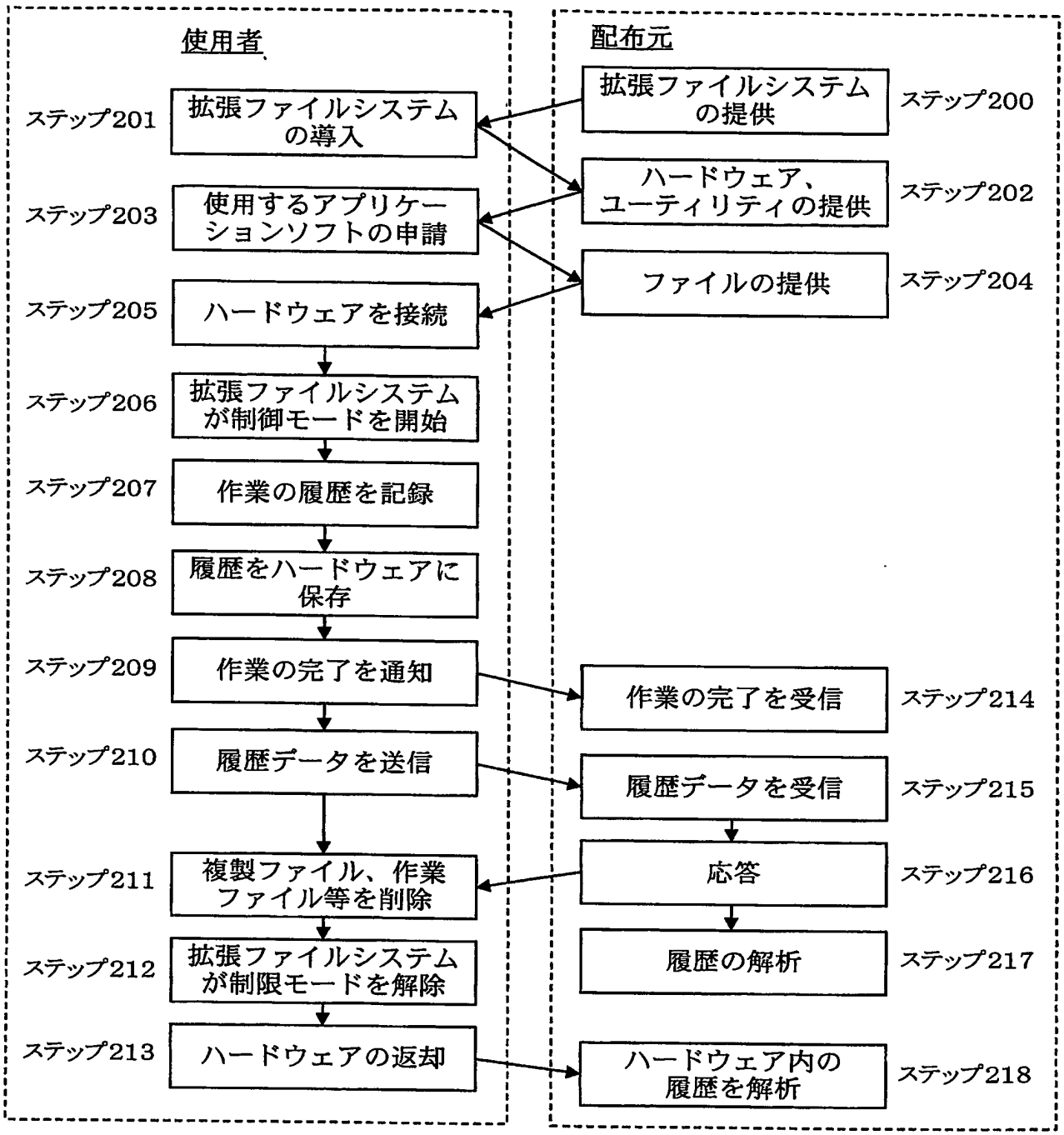
【図４】


スタート
USBコネクタで電子計算機と接続
ステップ10
ユーザの指紋認証
ステップ11
正当なユーザか？
ステップ12
いいえ
はい
PnP機能開始
ステップ14
制御プログラムのインストール
ステップ15
正常にインストールされたか？
ステップ16
いいえ
はい
利用許可がないユーザ
ステップ13
この電子計算機では利用できません
ステップ17
メモリスイッチの切り替え、第１メモリ利用可能にする
ステップ18
データの送受信
・
・
・
データの送受信
ステップ19
USBコネクター切断
ステップ20
電子計算機内のユーザデータを削除
ステップ21
インストールされた制御プログラムが消滅
ステップ22
エンド

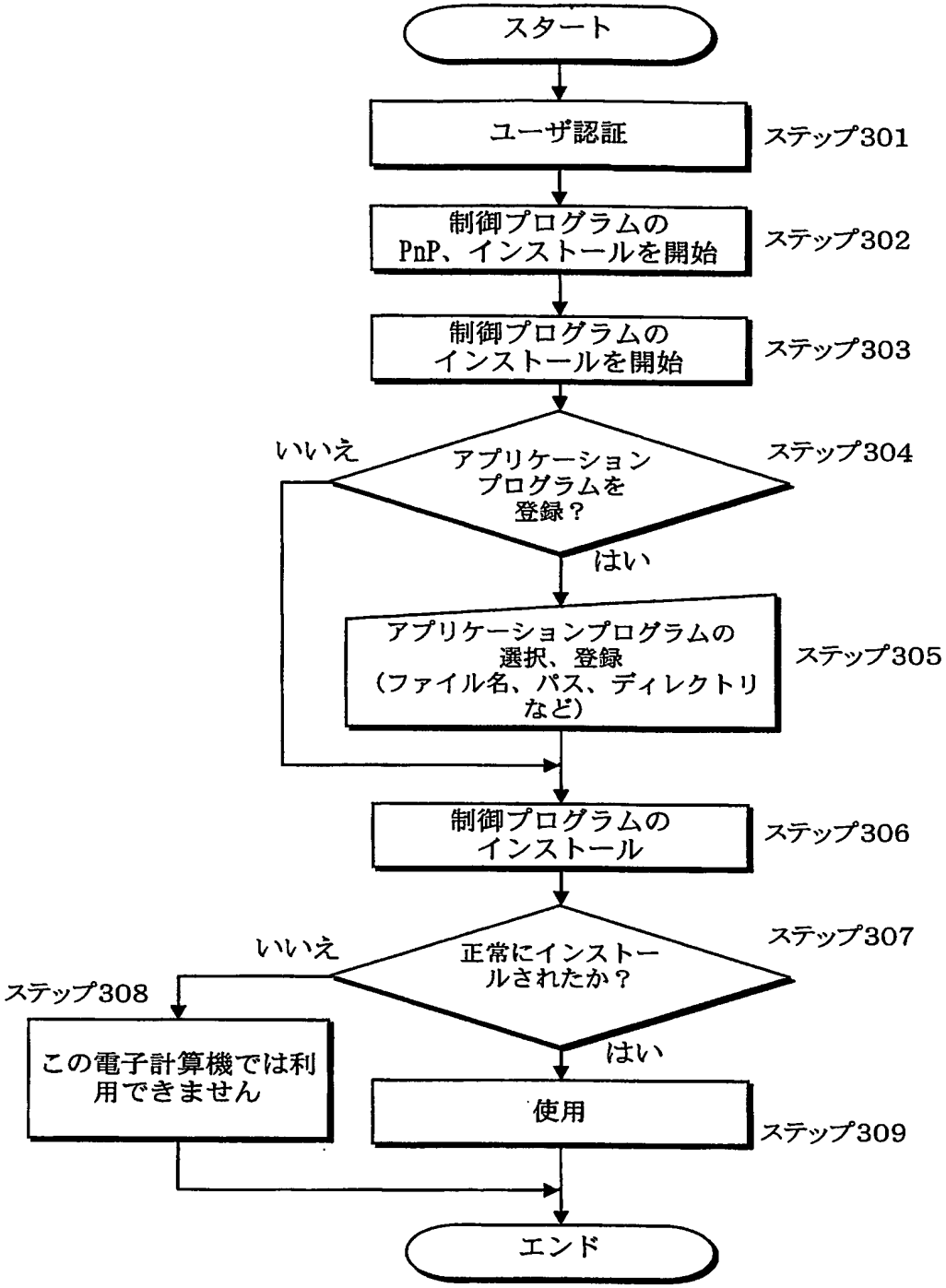
【図５】


スタート
USBコネクタで
電子計算機と接続
ステップ100
ステップ101
指紋認証
ステップ103
利用許可がないユーザ
ステップ102
正当な
ユーザか？
いいえ
はい
電子データ管理装置の
アンロック
ステップ104
メモリへのPnPの開始
ステップ105
データの送受信
ステップ106
USBコネクター切断
ステップ107
エンド

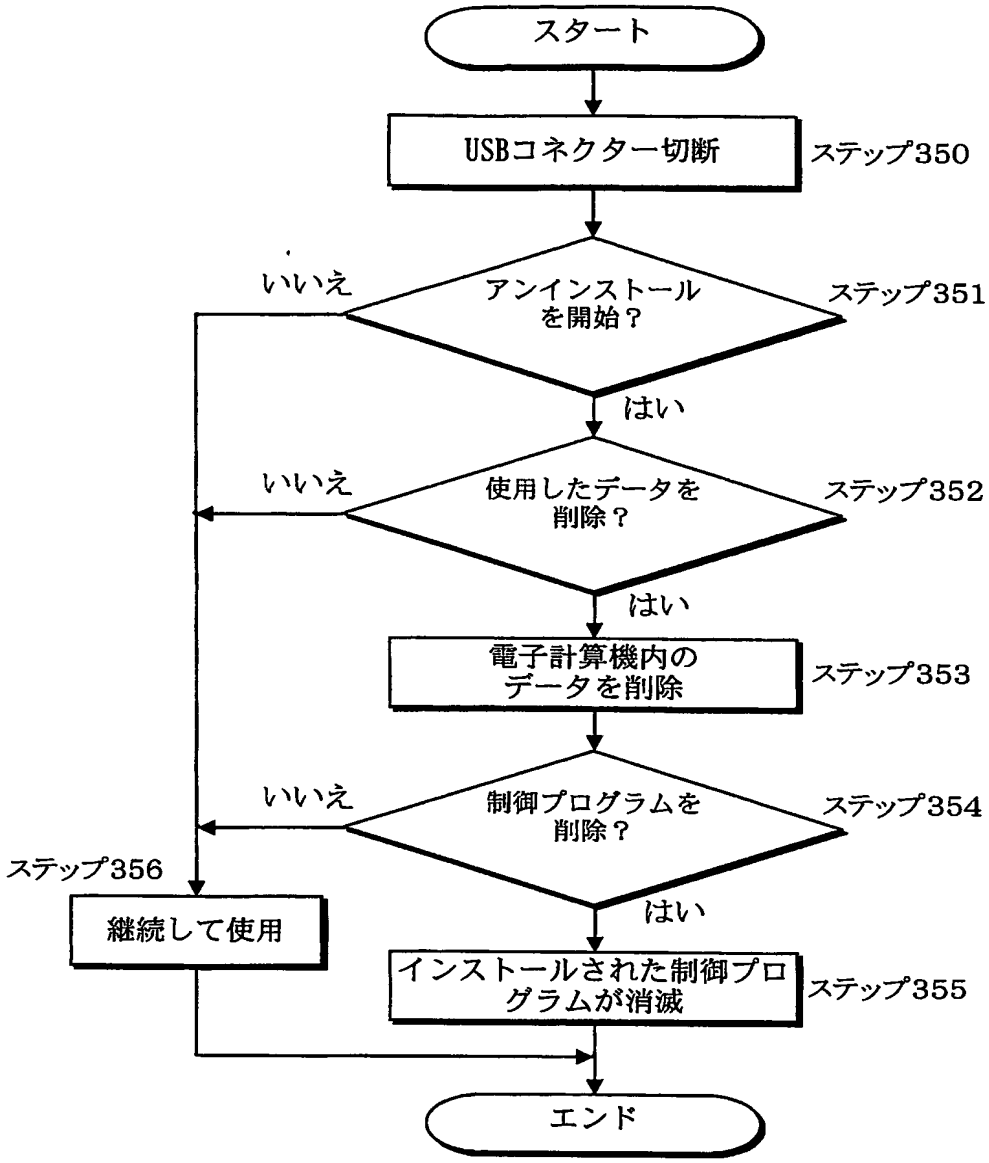
【図６】


使用者
配布元
ステップ201
拡張ファイルシステムの導入
ステップ200
拡張ファイルシステムの提供
ステップ202
ハードウェア、ユーティリティの提供
ステップ203
使用するアプリケーションソフトの申請
ステップ204
ファイルの提供
ステップ205
ハードウェアを接続
ステップ206
拡張ファイルシステムが制御モードを開始
ステップ207
作業の履歴を記録
ステップ208
履歴をハードウェアに保存
ステップ209
作業の完了を通知
ステップ214
作業の完了を受信
ステップ210
履歴データを送信
ステップ215
履歴データを受信
ステップ211
複製ファイル、作業ファイル等を削除
ステップ216
応答
ステップ212
拡張ファイルシステムが制限モードを解除
ステップ217
履歴の解析
ステップ213
ハードウェアの返却
ステップ218
ハードウェア内の履歴を解析

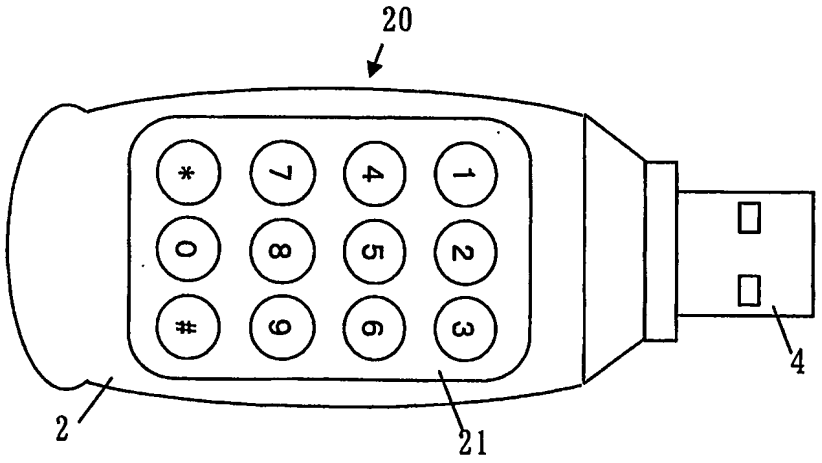
【図７】


スタート
ユーザ認証
ステップ301
制御プログラムの
PnP、インストールを開始
ステップ302
制御プログラムの
インストールを開始
ステップ303
いいえ
アプリケーション
プログラムを
登録？
ステップ304
はい
アプリケーションプログラムの
選択、登録
（ファイル名、パス、ディレクトリ
など）
ステップ305
制御プログラムの
インストール
ステップ306
いいえ
正常にインスト
ールされたか？
ステップ307
ステップ308
この電子計算機では利
用できません
はい
使用
ステップ309
エンド

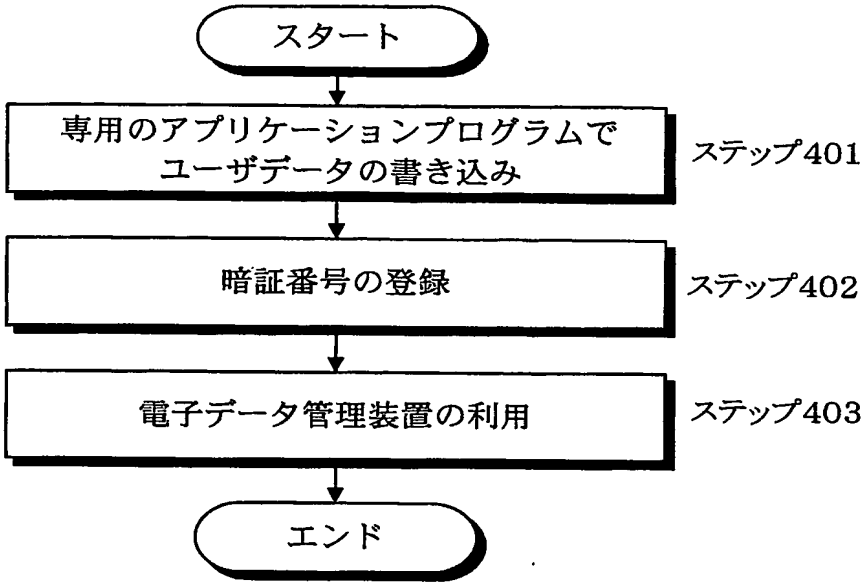
【図８】


スタート
USBコネクター切断
ステップ350
アンインストール
を開始？
ステップ351
いいえ
はい
使用したデータを
削除？
ステップ352
いいえ
はい
電子計算機内の
データを削除
ステップ353
制御プログラムを
削除？
ステップ354
いいえ
はい
ステップ356
継続して使用
インストールされた制御プロ
グラムが消滅
ステップ355
エンド

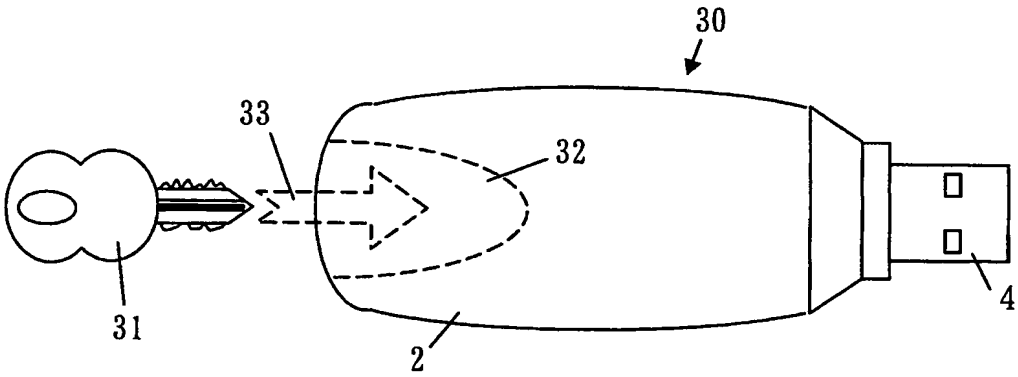
【図９】


20
*
7
4
1
0
8
5
2
#
9
6
3
2
21
4

【図１０】


スタート
専用のアプリケーションプログラムで
ユーザデータの書き込み
ステップ401
暗証番号の登録
ステップ402
電子データ管理装置の利用
ステップ403
エンド

【図１１】


30
33
32
31
2
4

【書類名】要約書
【要約】
【課題】電子計算機と接続されると自動的にインストールされて電子計算機内のデータの制御を行うことができる制御プログラムを格納した電子データ管理装置を提供する
【解決手段】電子データ管理装置１は、ユーザデータを記憶する第１メモリ６と、識別データが登録されている認証用データベース１１と、ユーザの認証情報を入力する入力部３と、入力部３からの入力データと、認証用データベース１１の登録された識別データとを比較してユーザの認証を行う認証モジュール１２と、電子計算機と接続して前記データの送受信を行うＵＳＢコネクタ４、制御プログラムを記憶する第２メモリ７を備える。ユーザ認証後、制御プログラムが電子計算機にインストールされ、スイッチ１０が第２メモリ７から第１メモリ６へと切り替えて、電子計算機からユーザデータを読み出しすることが可能になる。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２００３－２９４０５６
受付番号	５０３０１３５１９７４
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１５年　８月１９日

＜認定情報・付加情報＞

【提出日】　平成15年 8月18日

特願２００３－２９４０５６

出　願　人　履　歴　情　報

識別番号　［５０１１８０２６３］

１．変更年月日　２００１年　５月　７日
［変更理由］　新規登録
住　所　神奈川県座間市入谷４丁目３０１１番地の６　東建座間ハイツ２－５０９
氏　名　サイエンスパーク株式会社